UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Norfolk Division

STUDCO BUILDING SYSTEMS US, LLC,

Plaintiff,

v. Case No. 2:20-cv-00417

1st ADVANTAGE FEDERAL CREDIT UNION,
JOHN DOE,

Defendants.

PLAINTIFF STUDCO BUILDING SYSTEMS, US, LLC'S PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW

Plaintiff Studco Building Systems US, LLC ("Studco"), respectfully submits its proposed findings of fact and conclusions of law for the bench trial conducted on September 13-14, 2022:

I. STUDCO'S PROPOSED FINDINGS OF FACTS

A. Background on Studco.

1. Studco is a manufacturer of commercial metal building products for the wall and ceiling industry. Tr. 5:11-14.

2. Studco has been in business for 35 years in Australia and 16 years in the United States. Tr. 5:15-17.

3. To manufacture its metal building products, Studco purchases raw materials from suppliers. Tr. 5:18-21.

4. One of those suppliers is a vendor named Olympic Steel, Inc. ("Olympic Steel"). Tr. 5:22-23. Studco purchases raw steel coil from Olympic Steel. Tr. 5:11-6:1.

5. At the relevant time period, Studco had been buying from Olympic Steel for nine years. Tr. 6:2-4.

6. Olympic Steel's representatives visit Studco's offices every two to three months. Tr. 6:9-14.

7. Studco has a standard process to pay for orders with vendors like Olympic Steel. Tr. 6:16-10:11.

8. Studco's payment of vendor invoices goes through three levels of approval. Tr. 9:7-10. By utilizing this multi-tiered approval process, Studco ensures that no single individual or department can authorize transactions, which reduces the possibility of fraudulent payments being made to vendors. Tr. 9:15-10:4.

9. The purchasing process begins when Studco sends a purchase order to the vendor. Tr. 6:16-20. Once the ordered materials arrive at Studco's warehouse and Studco receives an invoice, Studco's invoice payment process begins with an accounts payable clerk matching the received items against the invoice and original purchase order. Tr. 7:2-11; 8:12-18.

10. After that occurs, the invoice is reviewed by the purchasing manager who initially placed the order. Tr. 8:18-21. The payment is then entered in Studco's computer system by accounts payable and sent to Studco's Global Managing Director, Ben Stevens, for final approval. Tr. 8:22-9:1.

11. Studco has also had a documented policy in place for changing a vendor's payment information since 2008. Tr. 10:16-11:6; Pl.'s Exs. 17, 18. Under the policy, only one, specified person in Studco's finance department had the authority to change the vendor's banking details in Studco's payment system. Tr. 12:20-13:2; Pl.'s Exs. 17, 18.

B. Studco's Information Technology ("IT") Systems and 2018 Security Incident

12. Studco utilizes a vendor – LMT Technology Solutions, Inc. ("LMT") – to maintain and monitor its information technology (IT) infrastructure. This vendor was working for Studco

in 2018. Tr. 14:6-12.

13. LMT provided Studco with monthly maintenance and security services. As part of that service, LMT performed system updates, managed firewalls, conducted network testing, and conducted employee training on phishing and spoofing attacks. Tr: 14:6-22. LMT also made recommendations on changes to Studco's internal policies to improve its security. Tr. 14:23-15:2.

14. Until September of 2018, Studco was never the victim of a security incident, including any intrusion of its computer systems, access by a malicious actor, or a disclosure of confidential information. Tr. 15:10-18.

15. Outside of the security incident in September 2018 (discussed below), Studco has not had any other security incidents. Tr. 15:19-22.

16. Studco attributes its lack of security-related incidents to its investment in internal controls and practices, and in leading-edge technology. Tr. 15:24-16:7.

17. Despite its implementation of industry best practices, Studco became the victim of unknown third-parties gaining access to its email system in September 2018. Tr.16:13-18.

18. Studco learned of the email intrusion on November 20, 2018. Tr. 16:13-18.

19. Upon learning of the intrusion, Studco immediately contacted its IT provider (LMT), its bank, its lawyers, and its insurance brokers. Tr. 16:25-17:9.

20. LMT immediately began investigating Studco's email system to determine how the third-parties accessed Studco's system, determined the extent of the third-parties' activities in Studco's email system, and removed the third-parties' access Studco's emails. Tr. 17:7-17.

21. In the course of LMT's investigation, it learned that unknown third-parties gained access to Studco's email system on September 24, 2018. Def's Ex. Tr. 34:21-25. Thereafter, these third-parties monitored Studco's communications, including communications between Studco and

its vendor Olympic Steel. Tr. 18:3-25.

22. The third-parties then intercepted legitimate communications between Studco and Olympic Steel, and then sent Studco a "spoofed" email on October 4, 2018. Tr. 35:12-36:6. Pl.'s Ex. 16. The spoofed email purportedly from Olympic Steel directed Studco to direct future vendor payments to an account at 1st Advantage Federal Credit Union ("1st Advantage"). Tr. 18:3-25. Pl.'s Ex. 12 at 2.

23. Olympic Steel had informed Studco before its receipt of the spoofed email that Olympic Steel would be sending Studco a change in banking instructions. Tr. 19:20-20:7.

24. Thus, Studco was expecting a change of banking information before it received the spoofed email. Tr. 19:20-20:7.

25. Following the instructions in the fraudulent email, Studco updated its vendor payment information for Olympic Steel to the 1st Advantage account. Thereafter, Studco's payments for invoices submitted by Olympic Steel were directed to that account through its vendor payment system. Tr. 19:9-25.

C. The Account at 1st Advantage

26. On or around August 9, 2018, an individual named Lesa Taylor ("Taylor") visited a 1st Advantage branch to open an account (the "Account"). Tr. 64:22-24.

27. At the time Taylor opened the account, she informed 1st Advantage that the account would be used for real estate transactions. Tr. 66:15-67:5.

28. However, Taylor's application to open the account stated that her occupation was a "merchant coord[inator]." Tr. 67:6-24; Pl.'s Ex. 19 at 1.

29. At the time Taylor opened the account, 1st Advantage was using a system called "Bridger Insight XG." Tr. 68:19-22. Bridger Insight XG is a software program that performs

identity verifications during account opening and checks whether the applicant is on the Office of Foreign Assets Control "Specially Designated Nationals" list. Tr. 68:23-69:8.

30. Discrepancies in the information Taylor provided to 1st Advantage while opening the new account triggered an ID verification alert in Bridger Insight XG. Tr. 69:9-18.

31. The alert caused 1st Advantage's compliance department to review the account information to approve the opening of the Account. Tr. 70:19-23.

32. Keith Ward ("Ward"), who was 1st Advantage's Compliance Manager and highest-ranking employee in 1st Advantage's compliance department was involved in the review of the ID verification alert on Taylor's account. Tr. 71:2-72:11; Pl.'s Ex. 7.

33. Despite the discrepancies and alert, 1st Advantage allowed Taylor to open the account (Account No. xxx713) (the "Account"). Tr. 74:9-12. The Account was a personal checking account, and not a business or commercial account. Tr. 68:16-18.

34. At the time Taylor opened the Account, she had two existing accounts at 1st Advantage: one she opened in 2010 (the "2010 Account") and one she opened in 2015 (the "2015 Account"). Tr. 77:12-22.

35. The 2010 Account had been active for approximately eight years as of the date Taylor opened her new Account in 2018. Tr. 77:23-78:1. In those eight years, the 2010 Account:

i. Never had a balance over $10,000;

ii. Never had a withdrawal of over $10,000; and

iii. Never had a deposit "anywhere near six figures."

Tr. 78:2-10.

36. The 2015 Account had been active for approximately three years as of the date Taylor opened her new Account in 2018. Tr. 78:11-14. In those three years, the 2015 Account:

i. Never had a balance over $10,000;

ii. Never had a withdrawal over $10,000; and

iii. Never had a deposit of six figures.

Tr. 78:11-20.

37. Notably, the 2010 Account and 2015 Account carried insignificant balances, around $1,000 or less, during their entire existence. Tr. 78:21-24.

38. In 2018, 1st Advantage received four ACH deposits originating from Studco and totaling $558,868.71 (the "ACH Deposits"). In particular:

i. On October 4, 2018 for $156,834.55.

ii. On October 16, 2018 for $246,260.44;

iii. On November 5, 2018 for $40,980.09; and

iv. On November 13, 2018 for $114,793.63.

Pl.'s Ex. 38; Stipulation of Fact 8; Tr. 76:13-21.

39. Mr. Ward admitted that the historical account activity in the 2010 Account and 2015 Account was "significantly different" than the five- and six-figure deposit and withdrawal activity in Taylor's new Account in October and November 2018. Tr. 78:25-79:4.

40. Each of the ACH Deposits:

i. Listed "Olympic Steel Inc." as the intended beneficiary (Tr. 76:25-3);

ii. Listed the Account number as the recipient (Tr. 76:25-3);

iii. Had a "CCD" code indicating it was a commercial or business-to-business transfer; and

iv. Generated a "WARNING" in 1st Advantage's systems notifying 1st Advantage of the discrepancy between the account holder name (Taylor) and name of the intended beneficiary (Olympic Steel).

Tr. 168:7-176:17.

41. Neither Studco nor Olympic Steel were customers of 1st Advantage. Tr. 266:9-18.

42. The Parties have stipulated that the following Table 1, demonstrates: (a) the monthly starting and ending balances for the Account, and (b) significant withdrawals and deposits by Taylor, between August 9, 2018 (when Taylor opened the Account) and December 31, 2018 (when 1st Advantage closed the account):

Date	Amount	Event
August 9, 2018	**$100.00**	**Starting Balance**
August 30, 2018	**$100.00**	**Ending Balance**
September 1, 2018	**$100.00**	**Starting Balance**
September 30, 2018	**$11.88**	**Ending Balance**
October 1, 2018	**$11.88**	**Starting Balance**
October 4, 2018	$156,834.55	ACH from "STUDCO BUILDING"
October 5. 2018	$58,000.00	Cashier's Check Withdrawal
October 10, 2018	$46,000.00	Outgoing Domestic Wire
October 12, 2018	$45,000.00	Outgoing Domestic Wire
October 16, 2018	$246,260.44	ACH from "STUDCO BUILDING"
October 17, 2018	$68,000.00	Cashier's Check Withdrawal
October 19, 2018	$79,500.00	Cashier's Check Withdrawal
October 23, 2018	$50,000.00	Withdrawal
October 25, 2018	$10,464.14	International Wire Transfer Attempted
October 25, 2018	$26,535.86	International Wire Transfer Attempted
October 30, 2018	$10,464.14	International Wire Transfer REVERSED
October 30, 2018	$26,535.86	International Wire Transfer REVERSED
October 31, 2018	$25,000.00	Withdrawal
October 31, 2018	$10,000.00	Withdrawal
October 31, 2018	**$1,282.90**	**Ending Balance**
November 1, 2018	**$1,282.90**	**Ending Balance**
November 5, 2018	$40,980.09	ACH from "STUDCO BUILDING"
November 6, 2018	$38,000.00	Cashier's Check Withdrawal
November 13, 2018	$114,793.63	ACH from "STUDCO BUILDING"
November 14, 2018	$60,000.00	Outgoing Domestic Wire

November 16, 2018	$45,000.00	Outgoing Domestic Wire
November 31, 2018	**$11.12**	**Ending Balance**
December 1, 2018	**$11.12**	**Ending Balance**
December 31, 2018	**$0.00**	**Ending Balance**

Pl.'s Ex. 38; Stipulation of Fact No. 9.

D. 1st Advantage's Anti-Money Laundering Software – Financial Crimes Risk Manager ("FCRM") Sends Multiple Alerts

43. The Bank Secrecy Act ("BSA") requires U.S. financial institutions (like 1st Advantage) to assist U.S. government agencies to detect and prevent money laundering, which includes reporting suspicious activity that might signify money laundering, tax evasion, or other criminal activities. Tr. 217:12-18; 224:12-225:7. To comply with BSA requirements, 1st Advantage relied on anti-money laundering software called "FCRM." Tr. 79:5-10.

44. FCRM is a "rules-based" software that monitored transactions in 1st Advantage's customers' accounts for suspicious activity based on pre-programmed rules in the software. Tr. 79:5-80:2. When a transaction triggered a rule, the software created an "alert." Tr. 79:20-25.

45. If a given transaction triggered an alert, 1st Advantage's analysts would investigate the alerts to determine what the next steps should be. Tr. 80:4-10.

46. In investigating the alert, the analysts would review past account activity, general account activity, and the accountholder's relationship with the institution. Tr. 80:11-22. However, historical account activity is "one of the largest factors in determining what the next action should be." Tr. 81:1-4.

47. The possible next actions for an alert included: (a) further monitoring, (b) opening a "case" to look deeper in the activity that generated the alert, (c) placing a restriction on the account, (d) closing the account, or (e) doing nothing. Tr. 81:5-82:1.

48. 1st Advantage had no documented guidelines to determine the appropriate next

action based on an alert. Tr. 82:2-19. Rather, when investigating an account, 1st Advantage made decisions on a case-by-case basis based on a "gut feeling" of the individual analyst. Tr. 82:9-19.

49. In any event, analysts would enter notes in the software about their decision on the appropriate next steps. Tr. 81:20-22.

50. FCRM was pre-programmed with rules (specific conditions) that would trigger an alert if a transaction "broke" a rule (*i.e.,* met the conditions in the pre-programmed rules). Tr. 84:13-17.

51. The conditions in the rules were designed around common factors indicating suspicious or criminal activity in the account. Tr. 85:22-24.

52. In a general sense, the purpose of the rules was to signal to 1st Advantage that something might be wrong in the account, Tr. 84:18-21, and give 1st Advantage an opportunity to investigate and resolve the suspicious activity in the account. Tr. 84:25-85:4.

53. Because the system is rules-based, the thresholds for triggering an alert were generally conservative because it was safer to have an alert and determine no further investigation was warranted (*i.e.* a false positive) than to have potentially fraudulent activity go undetected (*i.e.* a false negative). Tr. 85:5-9.

54. A certain transaction could trigger multiple alerts (*i.e.,* break multiple rules). Tr: 85:10-12.

55. 1st Advantage never made a change to the rules that came pre-programmed in FCRM. Tr. 85:13-19. Rather, 1st Advantage was using the "out-of-the-box" rules in FRCM. 85:20-22.

56. As of 2018, FRCM was one of the mostly commonly used AML software programs by credit unions in the country. Tr. 85:23-86:4.

57. 1st Advantage did not identify a noticeable issue with that FCRM's failing to trigger alerts for suspicious activity occurring in an account *(i.e.* with false negatives). Tr. 86:5-87:3.

58. 1st Advantage never conducted an analysis as to whether the thresholds in the FCRM rules were effectively set to detect suspicious activity. Tr. 87:4-11.

59. FCRM has a manual that sets forth all of the different alert types that are programed into the software. Tr. 88:4-22; Ex. 5 at 2-8.

60. FCRM would create an "alert" for the following types of transactions or patterns of transactions (among others):

A. ***High Product Service Activity***. This set of rules would trigger an alert if the account had a high value transaction or a high volume of transactions (deposits or withdrawals) using either cash, bank checks, wire transfers, or ACHs. Each rule in this category had a low, medium, and high threshold. The FRCM Manual indicated that evaluation of this alert required comparing other historical activity in the account. Examples of transactions that would create this type of alert included a customer:

i. purchasing large cashier's checks or a large volume of cashier's checks,

ii. attempting large domestic or international wire transfers or a high volume of wire transfers, and

iii. receiving or sending ACH transfers in a large volume or of large amounts.

Tr. 89:9-94:19.

B. ***New Accounts***. This rule would trigger alerts for all transaction types over a certain amount in new accounts (within 180 days of opening). FCRM had a rule specific to new accounts because the "greatest risk is in new accounts." There is a greater

risk in new accounts because (i) that is typically when accounts are used for improper purposes and (ii) the financial institution does not have an established relationship with the customer. Each rule in this category had a low, medium, and high threshold.

Tr. 94:20-97:8.

C. ***Pass-through Accounts***. This rule would triggers alerts if an account had "high balance turnover" (i.e. a customer putting a lot of money into an account and then immediately taking it out). This rule had low, medium, and high thresholds.

Tr. 97:9-23.

61. 1st Advantage could not identify the specific thresholds that would trigger an alert for any of the rules in FCRM. 98:9-12.

62. Based on 1st Advantage's description of the rules, the transactions in Table 1 would have triggered multiple alerts in FCRM. In particular, 1st Advantage agreed that:

i. Taylor's Account was a "new account" and that the six-figure balances in the new account should have triggered the new account alert. Tr. 97:5-8.

ii. The first ACH deposit from Studco on October 4, 2018 of $156,834.55 should that triggered a "high-product service" and "new account" alert. Tr. 103:1-9.

iii. Taylor's withdrawals on October 5, 10, and 12, which substantially removed the entire October 4 ACH within eight days of deposit, should have triggered the "pass through account" rule. Tr. 103:10-104:13.

iv. The second ACH deposit from Studco on October 16, 2018 of $246,260.44 should have triggered FCRM alerts. Tr. 104:14-105:11.

v. Taylor's withdrawals on October 17, 19, and 23, which substantially removed

the entire October 16 ACH within seven days of deposit, should have triggered FCRM alerts. Tr. 105:12-106:12.

vi. The third ACH deposit from Studco on November 5, 2018 of $40,980.90 should have triggered FCRM alerts for "high product service" and "new accounts." Tr. 105:23-106:12; 108:5-10.

vii. Taylor's withdrawals on November 6, which substantially removed the entire November 5 ACH within one day of deposit, should have triggered FCRM alerts for "pass through accounts" and "new accounts." Tr. 107:13-108:10.

viii. The fourth ACH deposit from Studco on November 13, 2018 of $114,793.63 should have triggered FCRM alerts. Tr. 108:11-25.

ix. Taylor's subsequent withdrawals, which substantially removed the entire November 13 ACH within three days of deposit, should have triggered FCRM alerts. Tr. 109:1-20.

63. Despite 1st Advantage testifying that FCRM was designed to and should have triggered alerts for numerous transactions in Taylor's account, Keith Ward, 1st Advantage's Compliance Manager, testified that FCRM "to his knowledge" did not trigger an alert. 109:21-110:14; 145:13-15.

64. Ward could not explain why FCRM did not trigger a single alert for Taylor's activity. Tr. 139:17-20.

65. Ward never reported the FCRM system as being broken. Tr. 149:13-14.

66. As of July 2019, 1st Advantage had:

i. Spoken with Studco's president Ben Stevens;

ii. Spoken with Studco's attorneys;

iii. Received letters from Studco blaming 1st Advantage for the loss of its funds; and

iv. Received an investigative subpoena from the Federal Bureau of Investigation ("FBI").

Tr. 111:14-112:4.

67. Around or after July 2019, 1st Advantage replaced FCRM with a new software through Verafin. Tr. 110:15-111:13.

68. As a part of replacing FCRM, 1st Advantage deleted all of the data stored in the FCRM system. 1st Advantage did not save the alert history or notes within FCRM when it deleted the data. Tr. 110:15-111:13.

69. FCRM's manual provided instructions on how 1st Advantage could export alert history from the system. Tr. 112:11-113:12; Ex. 5.

E. Taylor's Account Activity

70. Taylor made each of the withdrawals from the Account in the form of cashier's checks and wire transfers through an in-person transaction at a 1st Advantage branch. Tr. 131:5-11.

71. A "very small percentage" of 1st Advantage's customers have transactions of the size that were occurring in Taylor's account. Tr. 153:14-18.

72. 1st Advantage's tellers received training on detecting suspicious activity by customers. Tr. 131:12-14.

73. 1st Advantage's tellers are trained to "notify the proper individuals" if they "notice something" in the "normal processing" of a transaction. 1st Advantage could not articulate the

specific training that it provides its tellers, the frequency for that training or other information about the training. Tr. 131:19-25.

74. 1st Advantage's tellers had access to Taylor's account history and the document repository, Optical, when processing Taylor's deposit and wire transactions, cashier checks and other withdrawals Tr. 132:10-16.

75. Neither Ward nor anyone else at 1st Advantage reviewed the reports in Optical. Tr. 150:22-24.

76. 1st Advantage's tellers and managers review account history if they detect "suspicious activity" or "red flags" in a customer's transaction. Tr. 132:17-133:6.

77. On October 25, 2018, Taylor visited a 1st Advantage branch and attempted two international wire transfers totaling $37,000.00. Tr. 113:15-24.

78. The attempted wire transfers triggered an OFAC alert in 1st Advantage's fraud detection systems. Tr. 113:25-114:4.

79. The OFAC alert caused Taylor's account to be escalated to the compliance department. Tr. 114:10-115:11.

80. The OFAC alert caused 1st Advantage to question the purpose of Taylor's attempted international wires. Tr. 115:12-25.

81. Due to the OFAC alert and the suspicious nature of the two wire transfers, 1st Advantage cancelled the two wire transfers. Tr. 114:5-115:25; Pl.'s Ex. 8.

82. Following the cancellation of Taylor's October 25, 2018 attempted wire transfers, 1st Advantage made the decision to suspend "[a]ll wire transactions . . . pending further review." Tr. 117:2-8; Pl.'s Ex. 8.

83. Ward's testimony as to when he and the Compliance Department looked into Taylor's historical account activity on Taylor's account was inconsistent. *See* Findings of Fact 84-101, *infra*; Tr. 118:2-121:13.

84. Ward and the Compliance Department were involved in the investigation of the attempted Wires on October 25, 2018. Tr. 119:15-120:6.

85. During his deposition, Ward testified that "we" looked the historical account transaction during that investigation. Tr. 119:9-24. At trial, Ward said that "we" meant the Compliance Department, but not him personally. Tr. 119:25-120:5.

86. Ward testified that the Compliance Department "looked into all transactions in [Taylor's A]ccount." Tr. 120:2-8. *See also* Tr. 127:19-22 ("there was a look into the account to see other transactions . . . ."). Later, Ward testified at trial that the "primary focus at the time" was the attempted wires only. Tr. 152:9-14.

87. Ward testified that he did personally review Taylor's attempted wire activity on October 25, 2018, but he did not look at any of the other transactions in the Account. Tr. 152:3-16.

88. Taylor's attempted wires caused him and the Compliance Department to start an "ongoing investigation." 120:9-20.

89. As a part of that "ongoing investigation," Ward personally and the Compliance Department looked at Taylor's account "a handful of times" between October 25, 2018 and November 21, 2018. Tr. 121:3-5; 123:3-25; 277:17:278:7. Ward testified inconsistently, and also stated that he did not focus on the account anymore because he considered the "wire situation resolved." Tr. 152:19-153:3.

90. At all relevant times, Ward had ability to review the full transaction history in Taylor's account. Tr. 121:14-16.

91. Ward agreed that "historical transactions" are "one of the biggest factors in determining whether there is suspicious activity in an account. Tr. 124:11-19.

92. At all relevant times, Ward and the Compliance Department had access to "Optical," which was 1st Advantage's storage system for all of Taylor's account statements and member documents. Tr. 125:12-25.

93. During the handful of times that Ward looked into Taylor's account between October 25, 2018 and November 21, 2018, he looked at the account history in Taylor's account. However, Ward could not articulate the exact dates he reviewed that account history. Tr. 124:1-10; 278:4-16.

94. Ward did not create any documentation of his ongoing investigation of Taylor's account. 124:20-125:6; 129:7-11.

95. Ward agreed that when 1st Advantage was performing an investigation it was "best practice to get as much documentation as possible." 125:7-11.

96. At Ward's direction, 1st Advantage reversed the two fraudulent wires on October 30, 2018, but nevertheless permitted Taylor to withdraw $35,000 from the Account *the very next day*. Tr. 126:4-127:3.

97. Despite its ongoing investigation and placing a restriction on the account to suspend further wire activity on Taylor's Account, 1st Advantage allowed outgoing wire transfers on November 14 and November 16. Tr. 129:12-130:1.

98. Ward testified that 1st Advantage accomplished the account restriction requiring teller review prior to allowing a wire transfer through placing notices in its core system. However, 1st Advantage did not produce any evidence that such notes existed. Tr. 281:2-282:10.

99. 1st Advantage did not produce evidence showing it reviewed Taylor's account prior to Taylor's November 14 and 16 outgoing wire transfers despite the account restriction and the ongoing investigation. Tr. 282:1-13.

100. Ward could not explain why it was necessary to conduct an "ongoing investigation" if the only focus of 1st Advantage was to restrict further wire activity and 1st Advantage placing a restriction on Taylor's account. Tr. 129:1-8.

101. After October 25, 2018, 1st Advantage allowed Taylor to withdraw $178,000 from the Account. See Pl.'s Ex. 38.

F. The ACH Network and "Warnings"

102. The automated clearinghouse (ACH) system is a nationwide network through which depository institutions send each other batches of electronic credit and debit transfers. The National Automated Clearinghouse Association ("NACHA") Operating Rules direct how the ACH Network is operated.

103. It is the policy of 1st Advantage to conduct its ACH activities in compliance with the NACHA Operating Rules, Federal Reserve regulations, and Article 4A of the Uniform Commercial Code. Tr. 155:22-25; 158:17-Pl's Ex. 3 at 1.

104. Veronica Deans ("Deans") is the highest-ranking person in 1st Advantage's ACH department. Tr. 157:8-10.

105. Deans was the primary person responsible to ensure 1st Advantage was processing ACH payments within the NACHA Rules and other applicable guidelines. Tr. 156:4-8.

106. Deans was responsible for any questions related to fraudulent ACH payments. Tr. 157:8-11.

107. In 2018, 1st Advantage had a written policy related to processing ACH payments. However, that policy did not address how to handle misdirected payments or fraudulent ACHs. Tr. 158:1-160:2; Pl's Ex. 3.

108. 1st Advantage also did not have a system in place to monitor for fraudulent incoming ACH payments. Tr. 162:13-16.

109. 1st Advantage's ACH system will create an "exception" if something is "wrong with the transaction" and therefore requires manual intervention before 1st Advantage can post an incoming ACH to an account. Tr. 160:6-12.

110. 1st Advantage's ACH system also generated "Warning" reports. Tr. 160:16-18.

111. 1st Advantage's system would generate a Warning if the intended beneficiary of an incoming ACH did not match the name of the customer receiving the ACH. Tr. 162:17-22.

112. Each of the four incoming ACHs from Studco generated a Warning giving 1st Advantage knowledge of the discrepancy between of the name of the intended receiver (Olympic Steel) and the name of the account receiving the ACH (Taylor). Tr. 172:1-8; 173:16-23; 175:3-9; 176:10-17; Pl.'s Ex 2.

113. 1st Advantage's ACH policy did not address how 1st Advantage should handle "exceptions" or Warnings. Tr. 160:13-21.

114. The Warnings were generated contemporaneously (in real time) to 1st Advantage receiving the ACH containing the misdescription. 162:23-163:4.

115. The Warnings are saved in 1st Advantage's Optical system. Tr. 163:5-6.

116. 1st Advantage does not review the Warnings. Tr. 163:7-8;

117. The ACH department has the ability to review the documents Optical. Tr. 163:6-12.

118. Dean, the leader of the ACH department, could not explain why 1st Advantage has a system that generates Warnings only for them to be ignored. Tr. 163:16-21.

119. Deans was not aware of whether 1st Advantage's systems were capable of creating an "exception" when an incoming ACH's intended beneficiary does not match the name of the account holder receiving the ACH. Tr. 165:20-166:2.

120. Deans testified that the ACH system generates "hundreds to thousands" of Warnings per day. Tr. 177:15-25. However, Deans acknowledged that the ACH system creates multiple types of Warnings and no one at 1st Advantage actually reviews the Warnings. Tr. 179:5-10; 188:2-189:3. Thus, there is no way for Deans to know how many Warnings in the system are based on a misdescription between the name of the intended beneficiary and the account holder.

121. Each of the four incoming ACHs from Studco had a "CCD" classification which indicates that is corporate payment that is typically for business-to-business transactions. Tr. 169:15-170:1; Pl.'s Ex. 2.

122. The Warnings informed 1st Advantage of the mismatch between the intended beneficiary of the ACH (Olympic Steel) and the owner of the receiving account (Taylor). These Warnings gave 1st Advantage actual knowledge of the misdescription of the intended beneficiary of each of the four incoming ACH deposits from Studco.

G. 1st Advantage's Discussions with Studco and November 2018 Investigation

123. 1st Advantage did not restrict Taylor's account until November 21, 2018, after Ward received a call from Studco's President, Ben Stevens ("Stevens"). Tr. 133:7-134:9.

124. When Ward spoke to Stevens, he provided information that allowed 1st Advantage

to identify "the accountholder within 1st Advantage." Pl.'s Ex. 4 at 1.

125. In January 2019, Ward told 1st Advantage's attorney, Peter Katz, that the accountholder was involved in real estate. Tr. 134:21-135:1. Ward refused to provide the name of the accountholder because of "privacy" concerns. Tr. 21:22-23:9. At the time that conversation occurred, Ward had fully reviewed the transactions in Taylor's Account. 135:8-15.

126. Ward acknowledged that none of the transactions in Ward's account were related to an escrow company. Tr. 135:19-21.

127. Studco initiated this action on November 5, 2019.

H. Studco's Unrebutted Expert Testimony

128. Studco's Expert Witness, Elliott McEntee ("McEntee"), was qualified as a witness in the fields of risk management and ACH transactions at financial institutions without objection from 1st Advantage. Tr. 201:18-202:19.

129. Of relevance, McEntee has over 30 years of experience in risk management and ACH transactions at financial institutions. He was involved in creating the modern ACH system, and was involved in writing the NACHA rules as the former president of NACHA. Tr. 195:9-196:17; 198:7-19.

130. McEntee opined on three general topics:

i. the account opening process at 1st Advantage;

ii. the four-large value ACH deposits in Taylor's account; and

iii. the large value withdrawals from Taylor's account.

Tr. 206:16-207:1.

131. McEntee opined that based on the discrepancies at account opening, 1st Advantage should not have allowed the account to be opened or should have flagged the account as a

potentially risky account. Tr. 207:11-18.

132. McEntee opined that it was not commercially reasonable to allowed the ACH deposits in Taylor's Account. Tr. 208:20-209:16. The ACH Warnings "spelled out very clearly why [each of the incoming ACHs] were suspicious" and 1st Advantage "should have taken action, and . . . put a hold on the account." Tr. 209:6-12.

133. McEntee opined that not viewing Warnings because there are too many of them was not a good justification because the Warning system was a separate system that 1st Advantage paid for, and that 1st Advantage could sort out Warnings for high-dollar transactions that create the highest risk. Thus, ignoring the reports was not commercially reasonable. 211:3-15.

134. McEntee opined that the ACH rules allow financial institutions receiving ACH deposits to post a payment with a CCD classification in a personal account. However, it is not without risk because "there is something wrong with the transaction." Tr. 213:18-214:5.

135. McEntee opined that NACHA Rule 3.8.4 "requires a financial institution to return the transaction that they're not able to post because there's something wrong with the receiver's account." 216:25-217:3. Thus, 1st Advantage should have returned the ACHs from Studco with an RO3 code because Olympic Steel did not have an account at 1st Advantage. Tr. 217:4-9; 218:1-3. Pl.'s Ex. 27.

136. McEntee opined that it was commercially unreasonable for 1st Advantage to have allowed Taylor to withdraw the funds fraudulently posted to her account. 221:10-18. In 2018, there was tremendous publicity around individuals opening an account for the purpose of assisting in laundering money and moving it overseas. 221:21-222:5. The types of withdrawals used by Taylor – cashiers checks and wire transfers – were the type that should "create bells and whistles, alarms and red flags" because they are the "two main methods" used in money laundering. Tr.

222:6-23.

137. McEntee opined that the transactions in Taylor's account followed the "textbook" pattern of fraudulent activity and money laundering. Tr. 226:22-25. Based on his experience in risk management, McEntee opined that FCRM was designed to detect the types or patterns of transactions that occurred in Taylor's account and would have created multiple alerts. 227:1-9. The rules are programed conservatively to help the financial institution avoid risk. 228:19-25.

138. McEntee opined that 1st Advantage would have been justified in restricting the account after ***the very first ACH deposit on October 4, 2018***. Tr. 229:24-230:24.

139. McEntee opined that it was commercially unreasonable for 1st Advantage to not take an active role in determining the thresholds for the alerts in the rules. Tr. 235:1-9.

140. McEntee opined that 1st Advantage's tellers should be trained on detecting suspicious behavior from customer transactions with particularity. That would include looking at past transactions in the account, and providing tellers with protocols to follow. Tr. 235:18-236:17.

141. McEntee opined that it was commercially unreasonable for 1st Advantage to fail to restrict Taylor's account after her attempted international wires on October 25, 2018 initiated an internal investigation. 238:14-239:17; 263:10-20.

142. McEntee opined that it was not commercially reasonable for 1st Advantage to allow commercial deposits into a personal account. Tr. 262:3-13.

143. McEntee opined that it was not commercially reasonable for 1st Advantage to fail to review the historical account activity in addition to its automated processes. In particular, Ward should have looked past the attempted international wires on October 25, 2018. Tr. 262:14-263:8.

144. 1st Advantage did not proffer a rebuttal witness.

145. 1st Advantage did not proffer a witness as to the duty of or care or sufficiency of Studco's cybersecurity practices.

II. STUDCO'S PROPOSED CONCLUSIONS OF LAW

A. Studco's Spoliation Motion

i. The Court finds that 1st Advantage spoliated alert data in its FCRM Software

146. A party has a "duty to preserve" evidence in "reasonably foreseeable litigation" including preservation of information that the party "knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request." *Samsung Elecs. Co. v. Rambus, Inc.*, 439 F. Supp. 2d 524, 543 (E.D. Va. 2006), *vacated on other grounds*, 523 F.3d 1374 (Fed. Cir. 2008). *See also* Fed. R. Civ. P. 34.

147. "The obligation to retain discoverable materials is an affirmative one; it requires that the agency or corporate officers having notice of discovery obligations communicate those obligations to employees in possession of discoverable materials." *Samsung Elecs. Co.*, 439 F. Supp. 2d at 543 (quoting *Nat'l Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 557–58 (N.D. Cal. 1987)). The "duty to preserve" includes metadata if that metadata is relevant to the parties' dispute. *See E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc.*, 803 F. Supp. 2d 469, 496 (E.D. Va. 2011) (email fields).

148. "Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001) (citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir.1999)). "A court's power to sanction spoliation derives from two sources: (1) Fed. R. Civ. P. 37(e); and (2) its inherent power… to

redress conduct which abuses the judicial process." *Steves & Sons, Inc. v. JELD-WE/N, Inc.*, 327 F.R.D. 96, 103 (E.D. Va. 2018) (collecting cases)(internal citations omitted).

149. "[S]poliation of evidence is an abuse of the judicial process that is sanctionable under the inherent power" of the court. *Suntrust Mortg., Inc. v. AIG United Guar. Corp.*, No. 3:09cv529, 2011 WL 1225989, at *14 (E.D. Va. Mar. 29, 2011), aff'd, 508 F. App'x 243 (4th Cir. 2013). *See also E.I. du Pont*, 803 F. Supp. 2d at 499. "[T]he Eastern District [of Virginia] has endorsed the maxim that 'all things are presumed against a spoliator or wrongdoer.'" *Digital Vending Servs. Int'l, Inc. v. Univ. of Phoenix, Inc.*, No. 2:09CV555, 2013 WL 5533233, at *4 (E.D. Va. Oct. 3, 2013) (quoting *Trigon Ins. Co. v. United States*, 204 F.R.D. 277, 284 (E.D. Va. 2001)).

150. "[A] movant must satisfy four threshold requirements before a court decides if any spoliation sanction is appropriate: (1) ESI should have been preserved; (2) ESI was lost; (3) the loss was due to a party's failure to take reasonable steps to preserve the ESI; and (4) the ESI cannot be restored or replaced through additional discovery." *Steves & Sons*, 327 F.R.D. 96, 104 (E.D. Va. 2018).

151. The Court finds that 1st Advantage should have preserved the ESI in FCRM. "[C]ourts in the Fourth Circuit have found that the receipt of a demand letter, a request for evidence preservation, a threat of litigation, or a decision to pursue a claim will all trigger the duty to preserve evidence." *Id.* at 106. Ward agreed that as of January 2019, 1st Advantage had spoken with Studco's attorneys and received correspondences blaming 1st Advantage for the loss of funds deposited and withdrawn from Taylor's account. As of that date, 1st Advantage had notice of "reasonably foreseeable litigation" triggering its duty to preserve information that 1st Advantage knew or reasonably should have known would be "relevant in the action, … reasonably calculated

to lead to the discovery of admissible evidence, … reasonably likely to be requested during discovery, and/or … the subject of a pending discovery request." *Samsung*, 439 F. Supp. 2d at 543.

152. The Court finds that 1st Advantage lost the ESI in FCRM. Ward testified that FCRM was designed to and should have triggered alerts for the exact types of transactions that were occurring in the Account. Ward testified from his recollection that no alerts existed, but provided no reasonable basis to reconcile the two statements. Ward's recollection is not sufficient to establish that the ESI did not exist. In any event, 1st Advantage should have backed up the data in FCRM. The evidence showed FCRM had the capability to back up alert data, but 1st Advantage elected not to preserve that data. Accordingly, the Court finds that ESI in the form of "alert" data was lost when 1st Advantage deleted FCRM in July 2019. It is also likely that 1st Advantage lost notes of "cases" and investigation notes related to the Account when it deleted FCRM.

153. The Court finds that the ESI in FCRM's alert data was lost due to 1st Advantage's failure to take reasonable steps to preserve the ESI. Despite being under a duty to preserve and knowing that the data in FCRM would be relevant to Studco's claim, 1st Advantage made no attempt to preserve the FCRM alert data. 1st Advantage did not provide any evidence showing that preservation was not possible or would have been overly burdensome.

154. Finally, there is no dispute that the ESI cannot be restored or replaced through additional discovery. 1st Advantage has not offered any substitute means to obtain the lost data.

155. Accordingly, the Court finds that 1st Advantage spoliated relevant ESI in FCRM.

ii. The appropriate sanction for 1st Advantage's spoliation is a legal presumption in Studco's favor that the lost information was unfavorable to 1st Advantage

156. "In the Fourth Circuit, any level of fault, whether it is bad faith, willfulness, gross negligence, or ordinary negligence, suffices to support a finding of spoliation." *E.I. du Pont,* 803 F. Supp. 2d at 497 (citations omitted)(collecting cases).

157. Federal Rule of Civil Procedure 37(e) expressly addresses the imposition sanctions for the loss of "electronically stored information that should have been preserved in the anticipation or conduct of litigation . . . because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery."

158. Under Rule 37(e), the Court

> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

159. District Courts have a separate inherent power to sanction spoliation not addressed by Rule 37. *See Steves & Sons, Inc..,* 327 F.R.D. at 104.

a. FRCP 37(e)(2)

160. "'Destruction is willful when it is deliberate or intentional,' whereas bad faith destruction occurs when a party engages in destruction 'for the *purpose of depriving the adversary of evidence.'" E.I. du Pont*, 803 F. Supp. 2d at 497 (quoting *Powell v. Town of Sharpsburg,* 591 F. Supp. 2d 814, 820 (E.D.N.C. 2008)) (emphasis in original). *See also Buckley v. Mukasey*, 538 F.3d 306, 323 (4th Cir. 2008) (destruction of evidence, even if not in bad faith could still be willful).

161. 1st Advantage made an intentional decision to preserve some parts of FCRM – but not for Taylor's Account – after being put on notice of anticipated litigation by Studco. The disappearance of this data is particularly concerning considering that: (a) every other alert system employed by 1st Advantage triggered alerts from Taylor's account activity, and (b) the one system that 1st Advantage admits its manually reviews and should have produced alerts is missing. The circumstances surrounding the deletion of the data are sufficient to support the inference that 1st Advantage deleted the data with the intent to deprive Studco of that information.

162. The Court finds that the most appropriate sanction is to "presume that the lost information was unfavorable to [1st Advantage]." Fed. R. Civ. P. 37(e)(2).

163. Accordingly, Studco is entitled to a presumption that FCRM triggered alerts for each of the transactions set forth in Table 1, and that 1st Advantage's fraud analysts investigated each of those alerts under their normal process and discovered or should have discovered the fraudulent activity and stopped it.

b. FRCP 37(e)(1)

164. Alternatively, Studco is entitled to sanctions under Fed. R. Civ. P. 37(e)(1) because the loss of FCRM's alert data has prejudiced Studco's ability to prosecute its Misdescription of Beneficiary and Bailment claims against 1st Advantage.

165. The Court finds that the "measure no greater than necessary to cure the prejudice" is an order presuming that the lost information was unfavorable to 1st Advantage.

166. Accordingly, Studco is entitled to a presumption that FCRM triggered alerts for each of the transactions set forth in Table 1, and that 1st Advantage's fraud analysts investigated each of those alerts under their normal process and discovered or should have discovered the fraudulent activity and stopped it.

c. Inherent Authority

167. Finally, the Court has inherent authority to sanction 1st Advantage for its spoliation of FCRM data. *Goodman v. Praxair Servs., Inc.*, 632 F. Supp. 2d 494, 523–24 (D. Md. 2009).

168. For the same reasons set forth above, the Court finds that an order presuming that the lost information was unfavorable to 1st Advantage is an appropriate sanction. Accordingly, Studco is entitled to a presumption that FCRM triggered alerts for each of the transactions set forth in Table 1, and that 1st Advantage's fraud analysts investigated each of those alerts under their normal process and discovered or should have discovered the fraudulent activity and stopped it.

B. Misdescription of Beneficiary (Count I)

169. Under the Virginia Commercial Code, Studco has the right to recover the fraudulent ACH deposits that 1st Advantage received if Studco shows that 1st Advantage "[knew] that the name and [account] number" of the incoming ACHs from Studco "identif[ied] different persons." Va. Code Ann. § 8.4A-207(b)(1), (b)(2), and (d).

170. In other words, § 8.4A-207 required 1st Advantage to reject the ACH deposits if it knew that there was a misdescription between the intended beneficiary (Olympic Steel) and the owner of the account receiving the ACH (Taylor).

171. Section 8.4A-207 requires that 1st Advantage "know" of the discrepancy between the account name and number. The comments state that "Section 1-201(27) [provides the] rules for determining when an organization has knowledge of information." § 8.4A-207 cmt. 2.

172. The Virginia Code did not codify U.C.C. § 1-201(27) and the Uniform Commercial Code removed that section in the 1990 Amendment. U.C.C. § 1-201. However, the Virginia General Assembly's reference to former U.C.C. § 1-201(27) remains in the codified comments. § 8.4A-207. The Virginia General Assembly's failure to amend § 8.4A-207 to remove the

reference to former U.C.C. § 1-201(27) demonstrates that it intended the term "know" to be determined consistent with former U.C.C. § 1-201(27) definition.

173. Under the former U.C.C. § 1-201(27):

> Notice, knowledge or a notice or notification received by an organization is effective for a particular transaction from the time when it is brought to the attention of the individual conducting that transaction, ***and in any event from the time when it would have been brought to his attention if the organization had exercised due diligence***.

Id. (emphasis added). *See PAF Invs., LLC v. Gen. Dynamics Land Sys., Inc.*, No. 2:11-CV-552, 2012 WL 13005315 (D.S.C. Nov. 20, 2012) (applying UCC 1-201(27) to find that mail to organization's accounts receivable department provided actual notice); s*ee also Peter E. Shapiro, P.A. v. Wells Fargo Bank N.A.*, 795 F. App'x 741, 746 (11th Cir. 2019) ([UCC 1.201(27)] analog operates to impute organizational knowledge only when an organization fails to maintain "reasonable routines for communicating significant information" or fails to comply with those routines).

174. The Court finds that 1st Advantage had knowledge of the misdescription of beneficiary in the each of the four ACH deposits from Studco for three alternative reasons.

i. 1st Advantage had Actual Knowledge of the Misdescription from the WARNINGS in the ACH Items

175. First, 1st Advantage's corporate representative admitted that the "WARNINGs" in the ACH Items gave 1st Advantage contemporaneous "knowledge . . . that there is a discrepancy between the recipient name on the ACH and the name on the 1st Advantage account . . . ." This admission alone is sufficient to show that 1st Advantage had knowledge of the misdescription of beneficiary for each of the four ACH deposits.

ii. Alternatively, 1st Advantage had knowledge of misdescription under § 1-201(27)'s "reasonable diligence" standard

176. Under § 1-201(27), 1st Advantage obtained knowledge at the "time when [the misdescription] would have been brought to [1st Advantage's] attention if the organization had exercised due diligence." Under this standard, 1st Advantage is responsible for maintaining "reasonable routines for communicating significant information" in its software systems to the appropriate personnel. *See Peter E. Shapiro, P.A.*, 795 F. App'x at 746 (citing UCC 1-207(27)).

177. The Court finds that 1st Advantage should have established a "reasonable routine" for reviewing the Warning reports. Deans testified that it would be possible to review the alerts related to misdescription based on the volume. However, Deans also admitted that no one reviews the Warnings and the system generates multiple types of Warnings. Thus, she has no idea how many misdescription-based Warnings the system generates on a daily basis. On the other hand, Studco's expert testified that the system that generates Warnings is a module that 1st Advantage pays for, and that 1st Advantage could have designed a filter for high-value ACH transactions with a misdescription warning. The Court finds that designing that sort of filter would have been a reasonable routine to convey the important information in the Warnings Reports. If 1st Advantage would have done so the misdescription in each incoming ACH in Taylor's Account would have been brought to 1st Advantage's attention immediately and before Taylor could have withdrawn the funds. Under that standard, 1st Advantage had knowledge of the misdescription in each incoming ACH before Taylor's began her subsequent withdrawals.

178. Alternatively, the Court finds that 1st Advantage failed to establish a reasonable routine to detect suspicious activity in its customers' accounts. That suspicious activity included: (1) Taylor's suspicious account activity and alerts in FCRM, (2) Taylor's suspicious activity during teller interactions at in-person visits at 1st Advantage, and (3) Taylor's suspicious

international wires on October 25, 2018 that created an "ongoing investigation" by 1st Advantage's Director of Compliance. Studco's expert opined that the activity in the account was stereotypical suspicious conduct by an individual using an account for fraudulent purposes. A "reasonable routine" by a financial institution should have included proper systems and training to detect and stop Taylor's fraudulent transactions.

iii. Alternatively, 1st Advantage had knowledge of the misdescription under the "willful blindness" doctrine

179. Federal courts have imputed actual knowledge where a party remains willfully blind in an effort to escape liability in a variety of civil contexts. *See ePlus Inc. v. Lawson Software, Inc.*, No. 3:09CV620, 2011 WL 4704212 (E.D. Va. Oct. 4, 2011) (patent infringement); *Hard Rock Cafe Licensing Corp. v. Concession Servs., Inc.*, 955 F.2d 1143, 1148–49 (7th Cir. 1992) (Lanham Act); *Coach, Inc. v. Farmers Mkt. & Auction*, 881 F. Supp. 2d 695 (D. Md. 2012) (trademark infringement).

180. A willfully blind defendant is "someone who is playing ostrich to preserve a 'patina of innocence.'" *In re Mangrum*, 599 B.R. 868 (Bankr. E.D. Va. 2019) (quoting *Stoughton Lumber Co. v. Sveum*, 787 F.3d 1174, 1177 (7th Cir. 2015)). "A defendant acts with willful blindness if he 'subjectively believe[s] that there is a high probability that a fact exists' and 'take[s] deliberate actions to avoid learning of the fact.'" *ePlus*, 2011 WL 4704212, at *2 (quoting *Glob.-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011)).

181. As explained by Studco's expert, financial institutions pay for software and employees should read warnings and take action. 1st Advantage knew there was a high probability that the ACH Items' WARNINGs would inform it of the misdescription. Rather than review and take actions to protect consumers against fraud, 1st Advantage deliberately ignored those reports to avoid obtaining knowledge that might cause it to incur liability under § 8.4A-207.

182. Accordingly, the Court finds that 1st Advantage is imputed with knowledge of the misdescription under the "willful blindness" doctrine.

183. Because 1st Advantage had knowledge of the misdescription of beneficiary for all the reasons above, Studco has the right to recover the amount of the ACH deposits 1st Advantage received from Studco.

184. Accordingly, the Court enters judgment in Studco's favor and against 1st Advantage for $558,868.71 under Count I.

C. Bailment (Count III)

185. In the alternative, Studco is entitled to recover under its Bailment theory.

186. Under Virginia law, a bailment is "the rightful possession of goods by one who is not the owner." *K-B Corp. v. Gallagher*, 218 Va. 381, 384 (1977). A "bailee must use ordinary care for the protection, preservation, and return of the bailed property." *Volvo White Truck Corp. v. Vineyard*, 239 Va. 87, 91 (1990). The bailee is liable for the loss resulting from the bailee's failure to use ordinary care. *Id*.

187. "[T]he NACHA Rules and § 8.4A-207 UCC establish that 1st Advantage must act in a commercially reasonable manner or that it exercised ordinary care when it has control over ACH transfers." Dec. 18 Mem. Op. and Order at 11, ECF No. 41. "1st Advantage agrees that NACHA sets such a standard of care." *Id*.

188. 1st Advantage's receipt of Studco's ACH created a bailment.

189. 1st Advantage lost Studco's bailed property by allowing Taylor to withdraw Studco's funds from the Account.

190. 1st Advantage is responsible for the loss because it failed to act in a commercially reasonable manner or exercise ordinary care in each of the following ways:

A. First, Studco's expert opined that 1st Advantage opening Taylor's Account or at least not flagging the Account as potentially risky based on discrepancies during the account opening was not commercially reasonable. Failing to monitor the account upon opening led to Taylor using the Account for unchecked fraudulent conduct. 1st Advantage did not rebut this opinion. Studco's expert and Ward agreed that new accounts have the most risk because that is when the accounts will be used for fraud, and that Taylor's conduct followed the textbook pattern of fraudulent conduct.

B. Second, Studco's expert opined that 1st Advantage allowing the ACH deposits in Taylor's account based on the Warnings was not commercially reasonable. As explained above, Studco's expert opined that 1st Advantage should have been reviewing the Warnings and should have designed a filter to focus on the largest transactions. Studco's expert opined that the R03 code and NACHA Rule 3.8.4 required 1st Advantage to reject the ACHs. 1st Advantage admitted that the transactions in Taylor's account were very rare. Moreover, the ACHs were coded as CCD, which Studco's expert explained increased 1st Advantage's risk. 1st Advantage did not rebut this opinion.

C. Third, Studco's expert opined that 1st Advantage allowing Taylor to withdraw the funds fraudulently posted to her Account was not commercially reasonable. The pattern of deposits and withdrawals followed the "textbook" pattern of fraudulent activity and money laundering. 1st Advantage should have detected the suspicious activity during in-person teller interactions and through its FCRM software and placed a restriction on Taylor's account.

D. Fourth, McEntee opined that 1st Advantage failing to take an active role in determining the thresholds for the alerts in the rules in its FCRM software was not commercially reasonable. The record is unclear on whether the alerts existed: either (i) they did exist and were spoliated by 1st Advantage, or (ii) FCRM's rules were not appropriately set at thresholds that would effectively defect suspicious activity. Thus 1st Advantage either failed to effectively respond to alerts or had wholly ineffective software. In either case, 1st Advantage's conduct was not commercially reasonable and caused Studco's loss.

E. Fifth, McEntee opined that 1st Advantage's failure to review the historical account activity in addition to its automated processes after Taylor's attempted October 25, 2018 international wires was not commercially reasonable. 1st Advantage offered inconsistent testimony regarding what information Ward and the Compliance department were reviewing in Taylor's Account on October 25 and during the subsequent "ongoing investigation." Ward admitted that he and the Compliance Department eventually looked the historical account activity, and Taylor's account activity was suspicious. Yet, 1st Advantage did not place a restriction against further deposits or withdrawals. 1st Advantage's failure to reasonably investigate after October 25, 2018 allowed Taylor to withdraw an additional $178,000 from the account.

191. 1st Advantage's failure to act in a commercially reasonable manner or exercise ordinary care led to its loss of Studco's bailed property.

192. Accordingly, the Court enters judgment in Studco's favor and against 1st Advantage, in an amount equal to the lost property, for $558,868.71 under Count III.

D. Fraudulent Concealment (Count V)

193. The elements of fraud are: "(1) a false representation, (2) of a material fact, (3) made intentionally and knowingly, (4) with intent to mislead, (5) reliance by the party misled, and (6) resulting damage to the party misled." *Spence v. Griffin*, 236 Va. 21, 28 (1988). "[C]oncealment of a material fact by one who knows that the other party is acting upon the assumption that the fact does not exist constitutes actionable fraud." *Id.* "[W]illful nondisclosure of a material fact that [the defendant] knows is unknown to the other party may evince an intent to practice actual fraud." *Id.* "[C]oncealment is an affirmative act intended or known to be likely to keep another from learning of a fact of which he would otherwise have learned. Such affirmative action is always equivalent to a misrepresentation." *Van Deusen v. Snead*, 247 Va. 324, 329 (1994). The burden is upon the party charging fraud to prove it by clear and convincing evidence. *Id.* at 327.

194. Studco presented unrebutted facts demonstrating that 1st Advantage provided false information that hindered Studco's ability to recover its funds. 1st Advantage misleadingly told Studco that Taylor was a "business person" who was using the account to conduct a "high-value real estate transaction."

195. 1st Advantage had no basis for stating Taylor was involved in "high-value" real estate transactions and her own account history (which Ward had personally reviewed) showed the very opposite.

196. The Court finds that 1st Advantage knew or should have known those statements were false and were intended to hinder Studco from discovering that 1st Advantage's conduct had allowed the fraud to occur unchecked in Taylor's account.

197. These false representations damaged and hindered Studco's investigation of Taylor's fraud. These misrepresentations sent Studco on a goose chase in the hopes of discovering Taylor's identify and recovering against her purported real estate assets.

198. Separately or together, these facts are sufficient to demonstrate 1st Advantage's "affirmative act or representation designed to prevent, and which does prevent, the discovery of the cause of action."

199. Accordingly, judgment is entered in Studco's favor on Count III, in an amount equal to the lost property, for $558,868.71 under Count V.

200. Judgment is also entered in Studco's favor in amount equal to its attorneys' fees incurred by Studco as a result of 1st Advantage's fraudulent conduct. Studco is directed to submit a fee petition in support.

Dated: October 31, 2022

By: /s/Brett A. Spain

Brett A. Spain (VSB No. 44567)
Bethany J. Fogerty (VSB No. 94753)
Willcox & Savage, P.C.
440 Monticello Avenue, Ste. 2200
Norfolk, Virginia 23510
757.628.5500 Telephone
757.628.5566 Facsimile
bspain@wilsav.com
bfogerty@wilsav.com
and
Myriah V. Jaworski (admitted *pro hac vice*)
Chirag H. Patel (admitted *pro hac vice*)
Clark Hill PLC
1 Seneca Street, Suite 29
Buffalo, New York
360-901-9086 Telephone
mjaworski@clarkhill.com

cpatel@clarkhill.com
Attorneys for Plaintiff
Studco Building Systems U.S., LLC

CERTIFICATE OF SERVICE

I hereby certify that on the 31st day of October 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

/s/Brett A. Spain

Brett A. Spain (VSB No. 44567)
Bethany J. Fogerty (VSB No. 94753)
COUNSEL FOR STUDCO BUILDING SYSTEMS US, LLC
Willcox & Savage, P.C.
440 Monticello Avenue, Ste. 2200
Norfolk, Virginia 23510
757.628.5500 Telephone
757.628.5566 Facsimile
bspain@wilsav.com
bfogerty@wilsav.com